Fonds européen de développement régional (FEDER)
Europäischer Fonds für regionale Entwicklung (EFRE)

7.1.2: Report on the survey responses of electricity network operators in the three regions

Bushra Canaan, Djaffar Ould Abdeslam

Université de Haute-Alsace (UHA), Institut de Recherche en Informatique, Mathématiques, Automatique et Signal (IRIMAS)

1. Background and research gap

The sustainable development of the energy sector is based on diversification of energy resources, ensuring energy efficiency, affordability, and green energy production.

Both electrical networks operation control and sustainable energy transitions benefit from digitalisation. Simultaneously, the rapid expansion of distributed renewable energy resources and devices is increasing the connectivity and automation throughout the system which in turn is also increasing cybersecurity threats.

In the energy sector in general, cyber security is focused on ensuring reliability and resilience even in the case of a cyber-attack. A control system in the energy industry that is under attack, unlike IT systems, cannot be readily unplugged from the network since it could cause safety issues, brownouts, or even blackouts.

While it is impossible to completely prevent cyberattacks, energy systems can become more cyber resilient - able to endure, adapt to, and quickly recover from incidents and attacks while maintaining vital infrastructure operations. In order to ensure the cyber resilience of the whole power value chain, policymakers, regulators, utilities, and equipment providers all play critical responsibilities.

To harmonise the procedure among Member States and eliminate the weakest link problem in an interconnected energy grid, the European Union should facilitate the identification of operators of vital services. Specially to address the changing market conditions what might need to consider the emergence of new market players as operators of critical services. Therefore, under the recommendation of NIS Directive36, Member States are required to identify the operators of essential services [1].

In addition, and since information sharing can improve cyber resilience across the system, all stakeholders in the electrical sector should be encouraged to disclose information about vulnerabilities and actual incidents, to be honest about policies that have been enacted, and to share information and best practices at both the national and international levels.

2. Research goal and questions

Cyber resilience strategies necessitate action in linked industries like telecommunications and manufacturing, complicating the regulatory supervision process. Cyber resilience in the electricity sector should be considered as part of a larger effort to improve resilience across all key infrastructure and services, such as water, transportation, communication networks, health, and finance.

Many countries and businesses are creating and implementing rules and plans to improve their energy systems' cyber resilience. While different situations necessitate specialized approaches, a number of overarching action areas can serve as the foundation for future electrical security frameworks. Institutionalizing responsibilities and incentives; recognizing hazards; managing and mitigating risks; tracking progress; and responding to and recovering from disruptions are among them.

Confidentiality, Integrity, and Availability are three universally acknowledged protective goals in cyber security (CIA). The highest priority target in the energy sector is determined by the industry's specialised applications. The most significant factors in generation and transmission, for example, are availability and integrity as tampered or delayed data may cause a device to be misconfigured, posing a risk to system reliability. On the other hand, in advanced metering infrastructure the most important criteria is the security of customer personal data.

The fact that most countries' "traditional" electric grids have already grown into extremely complex networks adds to the technological obstacles of this shift. Limited operator investment has led in an aged infrastructure that is highly technical making it very difficult for regulatory authorities to design legal frames that could cover the following concerns:

- How energy is different from any other industry in terms of cyber security? And what are difficulties that need to be addressed in the energy sector?
- What are the recommended cyber security activities once the NIS Directive and GDPR have been completely implemented?

The purpose of this report is to explore the state of action of these topics in the context of the tri-national cross-border region of the Upper Rhine.

3. Research hypotheses

Experts believe that three criteria are required for a big cyberattack: opportunity, capacity, and motivation. The number of power outages caused by hacking has been minimal thus far. As the ability of attackers and the chance to attack (i.e. existing unaddressed vulnerabilities) grows, it is evident that electricity system stakeholders must remain well prepared and robust. Cyber resilience of the electricity system is becoming a subject of national security for countries all over the world.

Cyber resilience policies must be reviewed and adjusted on a regular basis. The risk exposure in the energy sector is shifting to the grid edge as decentralisation and digitization continues, particularly at the distribution level (smart meters, linked consumer devices). Effective policy must examine the entire electricity system, including supply chains, in addition to bulk utilities.

Supply chain security is a global concern. Certification or other equivalent procedures based on existing international standards must be institutionalized and interoperable at the global level, where considered suitable, to demonstrate security preparedness.

Despite the fact that most subsectors of the energy sector already have some measures in place, there is still an urgent need for these actions to be supported by a formalized and effective threat and risk management system.

However, because of the ambiguity and changing nature of cyberthreats, huge investments in people, tools, and cyber insurance policies are difficult to justify. Cyber risks in industry should be integrated throughout all departments (for example, operations, procurement, and innovation) and reported alongside other business-critical risks. It's crucial to create a cyber-resilient culture and strategy, starting with making sure that cybersecurity activities aren't limited to the IT department or the "cyber risk board."

4. Methodology incl. description of data

To define the energy sector demands, all parties engaged in the operation of energy infrastructures must be involved, primarily: Energy operators, which include all energy business units (generators, TSOs, DSOs, Suppliers, Aggregators, and Market Operators). As well as, industrial equipment suppliers who provide maintenance during the equipment's lifetime. In addition to, authorities/regulators who represent energy sectors. Not to mention, end users of the grids: consumers and prosumers, also consumer associations.

The analysis in this report was based on a literature review and interviews with some of the authorities involved in the project. RES-TMO has already engaged with a number of key stakeholders within the energy sector.

Face to face workshops were planned where discussions were used to elicit key needs & requirements from these stakeholders as well as to validate the content of this report. Unfortunately, most of these workshops have been transformed to online event due to covid-19 crisis restrictions.

In the following a brief representation of the workshops that we attended either as observatory partner from the RES-TMO staff, representators or even organizers. Our interventions mainly revolved around introducing the cyber-Physical security aspect as an emerging challenge to encounter in the new energy systems and set a platform for initiating discussions and spreading awareness

5. Attended Workshops:

Stakeholder Workshop: Energy Citizen-based renewable energy, emergence of a local project: challenges and levers for action (Strasbourg 23/09/2019)

The workshop in partnership with WP4 was dealing with the issues raised by energy citizen and cross-border cooperation. This event, held in Strasbourg, brought together about thirty participants from the three national areas of the Upper Rhine working on renewable energy at different levels: representatives of citizen cooperatives, local authority representatives and members of associations.

It focused on citizen-driven cooperative initiatives on energy and was organised by the SAGE laboratory of the University of Strasbourg and the coordination office in collaboration with Alter Alsace Energies and the GECLER network (Grand Est Energie Citoyenne).

Community action and involvement in the transition towards a society based on sustainable renewable energy has increased significantly during the last decade, leading to changes in how energy systems are integrated into societies around the world.

The workshop resulted in fruitful discussions on citizen energy, with participants delving into the regulatory, financial, institutional, and operational challenges of citizen-based clean energy cooperative initiatives in the three national contexts, as well as the opportunities offered by cross-border collaboration.

In our turn, we raised the question about energy security and the acceptability issue that encountering the enrolment of smart meter across the three countries. Especially when utilities condition the presence of smart applications and intelligent metering infrastructure for an efficient, secure, and reliable transit towards higher shares of Renewable Energy Sources (RES) and smart grids.

We also discussed in smaller groups the role that these communities could have in the decision-making mechanism under the growing concerns about confidentiality issues.

Stakeholder Workshop: Citizens as Prosumers: Legal Status, Rights, Involvement in the Energy Transition (07/10/2020)

In the same way, the second workshop was held online on October 7, 2020. It was organized under the collaboration between partners from WP4 and WP5, the social and legal scholars involved in the RES-TMO program. The workshop delt with regulatory issues and the new role of citizens as prosumers.

The development of renewable energy depends to a large extent on the commitment of local political, economic, and social actors that assigns new roles to citizens that produce and consume their own renewable energy. The growth of European prosumers is challenging existing energy market structures and institutions. And while the municipalities or groups of municipalities at the territorial level favourite the development of these projects, the national context – regulations and financial aids – are often responsible for decelerating the launching of new projects.

The key participants in this workshop have underlined the crucial role played by national states, German Länder, and Swiss cantons in forming the main incentives which could take the form of new regulations or financial measures such as feed-in tariffs in this area.

Since local actors need to examine and exploit the regulatory background, as well as the evolution of taxes when implementing their projects, they possess a certain awareness of the application of these latter. At the same time, when it comes to European legislation and standards, they are less familiar with them and more often lack expertise and in-depth understanding of the application of these norms.

Intermediate levels, expressed in urban planning papers or local, mostly regional, financial support from the départements in France, the Länder in Germany, and the cantons in Switzerland, can supplement the European, national, and territorial levels. With dedicated services and agents, local governments are getting increasingly active in energy concerns (such as a Klimaschutz manager in Germany or an energy transition officer in France, for example).

Our Participation has evoked the discussion on the legal feasibility of adopting prosumer communities and microgrids models as a solution not only for facilitating the integration of small to medium scale RES but also as an approach to enhance regional resiliency and security.

From a French point of view, self-consumption regulations were incorporated into the French Energy Code In 2015 and 2016. The 2015–992 Energy Transition Law and the 2016–1019 Self Consumption Ordinance, which regulate individual and community self-consumption, are the most essential legal provisions. Electricity producers and users must have access to the system, which is regulated by the Energy Regulatory Commission, on an equal and non-discriminatory basis[2].

Self-consumption is collective when electricity is provided between one or more producers and one or more final consumers who are tied (among themselves) within a legal structure of a legal person, located in proximity, and whose extraction and injection points are located after the same low-to-medium voltage transformer station, according to the Energy Code (Art. 315).

Civil Society Organizations (CSOs) can generate and sell their renewable energy. They may (or may not) benefit from particular assistance schemes, depending on the size of the project:

According to an expert interview conducted by [3] in 2018, Except if they profit from the feed-in tariff (FIT), CSOs are allowed to participate in energy markets. A CSO that receives a fixed FIT would not be active on the market; the company that purchases their energy would be responsible for all market-related activity.

Small installations of up to 3 kW have the option of donating energy to the grid. For projects under 36 kW, all CSOs can benefit from an investment premium and a FIT, as well as tenders for larger projects (above 100 kW) and various grid prices and tax deductions. According to one respondent (November 2018), the payment for a CSO's surplus energy is made based on a contract that ties the community's members.

During the same interview, the fact that CSOs are excluded from the responsibilities of energy suppliers was highlighted stressing that They could decide to register as an energy supplier if they wish. Nonetheless at this case, they would be held to high and demanding standards, including balancing responsibility, as well as technical and financial capability.

On the other hand, even though that Renewable Energy Communities (RECs) have no legal definition, they still may take the legal form of a CSO. It is possible also for Residents of multi-apartment buildings or condominiums to claim the same legal model where it can exchange surplus energy between each other and correspondingly become jointly acting self-consumers. Other entities like Citizen energy communities (CECs) could be of cooperative nature even if it does not implement the legal form for CSO.

In Germany, The legislation that depicts the prosumer role on the German side is the Renewable Energy Sources Act 2017 (EEG), As it describes self-consumption behaviour and characterizes the energy community which is cited as 'Citizen Community'[4]. It stipulates that Renewable energy must be prioritised by the grid operators. Directly or through aggregators, all forms of self-consumers can participate in the energy market.

This was confirmed through expert interviews also from [3], which explained that service companies/suppliers or aggregators hosting energy communities have the possibility to directly sell the electricity produced by these communities under their name or as a white label product with the name of the involved community. Knowing that both energy communities and energy providers are subjected to the same regulations making it hardly profitable for small scale communities.

In addition, a registration as an energy supplier with an official permit is required in terms to be able to take a part in the market directly. At the same time, some argue that this process could be quite complicated from an administrative viewpoint and prohibitively expensive.

Different renewable power plants receive different compensation modalities based on the size of the installation measured in overall capacity in kW. For example, the market premium feed-in tariff ranges from 10.28 cents (<100 kWp) to 11.83 cents (<10 kWp) for each kWh, while for all installed capacities that is equal or exceed the 750 kW should enter a public tender.

Also, according to EEG 2017 Tenant Supply Act (Mieterstrom), electricity sharing within neighbourhoods and buildings that include multiple apartments is legally feasible. When a building owner is registered a licensed supplier, he or she becomes able to sell electricity generated from roof top photovoltaic panels to his tenants.

The act establishes standards for the term of the contract governing the delivery of electricity from a landlord to a tenant, prohibits landlords from including this contract in the rental agreement, and places a limit on the amount landlords can charge renters for the electricity they provide.

Regarding the electricity surplus injected into the grid, lessees benefit from a similar feed-in tariff remuneration. In parallel, they are charged an additional 'tenant-electricity surcharge' for their self-consumed energy. while they must pay 40% of the EEG apportionments earmarked for conventional power customers[4].

Furthermore, the act includes a legal definition of the energy community concept (Bürgerenergie) in terms of financial participation via equity in a RE installation that distinguishes Germany from every other member state.

The term Bürgerenergie translates literally to citizen energy or Citizen Community. The voting process in these communities necessitates that at least 51% of voting rights should be assigned to natural persons from the district that contained the energy-producing plant including non-renewables, resulting in communities that can have the characteristics of both the REC and the CEC concepts.

It is worth mentioning that some incentives were specially addressed for RECs. where it's possible for them to take a part in wind tenders with project size limited to 18 MW (6 turbines). Local authorities also are eligible to invest with a percentage that could reach 10% in these projects. Before 2018, RECs were privileged to take a part in the tendering procedure without permits ahead of other participators[5]. Although federal rules (such as the EEG) and federal money have had a significant impact on renewable energy deployment in Germany, federal states (Länder) also give significant assistance to renewables. Some Federal States allocate RECs with support schemes with a geographical variance in levels of support since some states have been more engaged than others. While the most effective federal instruments of assistance are focused on the use of renewable energies for electricity generation, the promotion of renewable technologies on a regional/state level is focused on heating and cooling. Furthermore, regional support is frequently focused on a single industry. One federal state-run programme, for example, specifically helps agriculture. Photovoltaic and biogas systems receive the most support from regional initiatives and, as a result, make the most money. While federal funds or federal law have been the primary engine for the deployment of renewable energy technologies, the federal states (Länder) have also contributed significantly. There have been some states that have been more active than others[6].

In conclusion, compared to other member states Germany's regulatory framework for collective prosumers appears to be stronger, without necessarily being the most financially advantageous in all the reforms. Which has been emphasized in [3] during an expert interview in 2019, by stating that multiple modifications in the EEG 2017 law had made it an extremely complex statute, resulting in a complicated legislative structure and frequently resulting in additional unanticipated expenditures for prosumers.

Stakeholder Workshop: Regional energy resilience and decarbonization through decentralized RES: pathways, technologies, regulations, challenges (10/11/2020)

the workshop hosted representatives from Fraunhofer Institute for Solar Energy Systems (ISE), the energy service provider and distribution grid operator Badenova and The French multinational electric utility company (EDF). In addition to 26 regional energy stakeholders from France, Germany, and Switzerland.

Expert presentations have covered key themes in terms of energy system transformation pathways and flexibility options, Viable energy storage technologies – batteries vs. hydrogen using existing gas infrastructures, and related material and energy needs.

These presentations were followed by an interactive session in which participants had open discussions in smaller groups. Dr. Djaffar Ould Abdeslam has animated one of the two working groups. Wherein, the focus was on technical challenges of regional resiliency concerning the effect of increasing distributed renewable resources on managing demand response mechanisms on local and regional basis. Namely with a reflection on electricity security in the context of intensified dependency on low inertia systems while ensuring adequacy and available reserves. Along with the role of storage systems available technologies, models and requirements in supporting the tendency towards decarbonizing the Energy sector.

On the French side, the electricity system is already considered a low-carbon sector due to nuclear generation. Yet these plants will soon reach the limits of their lifespan leaving France with only two possibilities that obligatorily imply a greater share of Renewables in order to respect its commitments to the energy and climate law and the National Low-Carbon Strategy (Stratégie nationale bas-carbone, or SNBC)[7].

For Germany, sector-coupling especially in the case of connecting the transportation and heating sectors to the power sector is deemed an important element in the energy transition that results in different implications for the energy system transformation pathway. Simultaneously, power generation from offshore wind farms is expected to take a vital part in the future power system replacing medium-load fossil-fuelled power plants, notably with their elevated load factors and a predictable cost reduction. which in turn implies the importance of large-scale energy storage deployment needed for a successful energy transition[8].

According to[9] France needs to strictly stick to the following recommendations for a secure introduction of very high shares of RES. First, maintaining system stability without conventional generation assets is a notion that receives a general scientific consensus. Despite the anticipated impact of integrating an important share of distributed solar PV which may produce difficulties in supply security, these arguments need to be profoundly assessed before adopting them as a pretext that holds back the power sector from hosting more DRS.

Second, for ensuring a fundamentally renewable-based system's ability to handle loads at any given moment which is known as system adequacy, substantial flexibility sources, in particular, considerable storage capacities, peak load generation, demand response management mechanisms and an advanced transmission networks are required.

Operational reserves scale and renewables forecasting approaches accompanied by regulatory frameworks responsible for the trade-off between obligation that needs to be fulfilled and procurements should be reviewed and readjusted on a regular base.

Moreover, robust proactive measures, involving the public in the long-term provision, costs analysis and working with citizens on social acceptance is very essential for sustainable grid development not only towards a new architecture of the grid but also to accompany the process of replacing the ageing assets. Not to mention that working on a regional scope call for even more multi-services interoperability for further exploitation of local potentials.

These conditions for smoothening the transit to a more resilient and decarbonized power grid could be generalized to work for any country with the same fixed objective.

Stakeholder Workshop: Regional energy resilience via distributed RES and the role of smart grids: challenges and opportunities (cyber security) (04/05/2021)

In collaboration with WP1, and TRION-climate, we have organized a workshop mainly based on the underlying concept of the WP7 of the project (Data security through smart grids). The event has started by offering a brief introduction to the multidisciplinary nature of the work package. All along with explaining the motivation behind the recent integration of the cyber-physical security aspect as a pillar for energy system security, regional resiliency and technology enrolment public acceptability. Followed by an elaborated presentation of our technical contribution on detecting cyber attacks in connected microgrids using real-time digital simulator provided by our partners from Opal RT. A demonstration of the lab's small microgrid was also prepared for highlighting the importance of adopting these schemes in pursuing local resiliency and the practical application of the proposed method.

A series of private sector expert presentations followed. The first stakeholder presentation was given by Mr. Mohamed Hamdani from ENEDIS, the French distribution system operator (DSO). ENEDIS actually manages 95% of the public electricity distribution network in France. Mr. Hamdani explained how smart grids opened up new possibilities for DSOs and their clients because of the large-scale rollout of smart meters across France that is expected to reach almost 80% of French consumers by 2022. The smart meters collectively generate a huge amount of data, which can be aggregated to help cities better manage their energy consumption. For example, ENEDIS has helped the city of Mulhouse develop strategic renovation plans by ranking buildings according to their energy use and assisted cities such as Saint Louis to better allocate EV charging points. The spread of smart meters also makes it easier for DSOs to identify and resolve issues in the grid consequently reducing outages.

The second expert presentation was given by Ms. Carmen Exner from Netze BW GmbH, a German DSO operating in the federal state of Baden-Württemberg. Ms. Exner coordinates the flexQgrid project, which aims to efficiently integrate decentralized generation into the distribution grid. The project makes use of a traffic light system concept that connects all actors (such as PV modules, charging stations, etc.) and indicates how they should adapt their energy consumption based on grid congestion forecasts. The project includes a real time case study and field tests over the period of three years in the town of Freiamt.

Mr. Daniel Blättler from Primeo Energie, a Swiss energy provider, was the last guest speaker. Mr. Blättler focused on the data security of smart metering systems. He elaborated on three key issues – confidentiality, integrity and accessibility – which are closely regulated by national and international standards. The adopted approach is to take preventative actions to avoid problems, including deploying sophisticated programs to detect attacks and lifecycle management systems to prevent the manipulation of smart meter chips. Ultimately, however, attacks are often linked to human error, which is more difficult to prevent.

After each of the three presentations, the participants asked a multitude of questions which resulted in a series of engaging discussions with the three guest presenters. The workshop ended on a positive note after the last stakeholder presented and the discussion promptly ended.

Informal interviews and discussions with experts within the consortium

Two preliminary meetings were held with representatives from the French distribution operators Enedis and the transmission operators Rte on the matter of data availability and adopted security strategies namely concerning the French smart-meter Linky. Discussion evoked existing and arising challenges with a brief reflection on future perspectives.

We also arranged the meeting with the mayor of Ungersheim, Jean-Claude Mensch and evoked discussion about their opposing position to the French smart meter Linky.

In a meeting with Mr. Mohamed Hamdani (Directeur Délégué Aux Affaires Territoriales Le réseau au service de la transition écologique Enedis)

The discussion covered the role of the DSOs in the increased penetration of DERs and, challenges emerging from the adoption of smart and connected features in addition to the adopted data sharing strategy. Which in turn has imposed the new role of communication and information service manager to be assigned to the Distribution network operator.

Enedis allow controlled and secure access to data. It provides service developers with several data services such as Data Connect (Linky API platform), SGE (the data exchange platform for electricity market players), Dataconsoelec (the ad hoc data request service), and Tele-information (remote display and equipment control) that enables customers to share their energy data with service providers.

Stressing the fact that these tools enabled by the Linky communicating meter is essential for achieving the ecological transition and facilitating the development of renewable electricity as it offers a more accurate view of the electricity network on a daily basis and of the consumption and production Through better control of energy demand, it also contributes to the development of electric mobility

Knowing that, Enedis became the first European utility to publish aggregated energy data in Open Data In 2015. Open Data consists of making data freely available for consultation by all citizens. It is about making data available to all, in a simple, downloadable and reusable format, thanks to IT tools that allow their reuse by any authorized actor who wishes to do so.

Consumption and production, description of the electricity network or overview of renewable energies, these data that we publish are useful to actors as varied as local authorities, service providers, electric mobility actors, associations, electricity market actors, researchers or even citizens, in particular in order to better understand the energy transition, its stakes and its implications.

Of course, Enedis protects personal data (DCP) and commercially sensitive information (ICS). Consumption and production data, for example, take into account the aggregation rules set by the regulations. No individual data of a particular customer can be published in Open Data.

6. Results

Policymakers and regulators must play a key role in promoting cyber resilience measures. Adding cybersecurity criteria to the rate base for regulated electricity grid operators, or qualification criteria to stakeholders participating in the market or connecting directly to the grid, are examples of regulatory requirements that can help ensure that the minimum necessary investments are made. Compliance with regulatory standards, on the other hand, does not guarantee that infrastructure is or will be totally secure and robust. In general, regulatory norms may struggle to keep up with rapid technology change and growing vulnerabilities due to decision-making processes and the requirement for stable and inclusive governance.

Within their domain, policymakers must establish suitable responsibilities and incentives for relevant organizations. They also shall be competent for appointing responsible authorities to formulate goals, direct measures, and evaluate their implementation. Implement coordination procedures amongst competent authorities (both within and outside the energy sector) to avoid disputes between multiple regulatory levels, according to policymakers and regulators.

They should incentivize or compel regulated and non-regulated firms to install cybersecurity protections. Rather of depending solely on compliance-based processes that risk becoming a box-ticking exercise, measures should attempt to improve results. The severity of sanctions should be proportional to how important the organization is to overall system reliability.

To promote transparency, cooperation, and coordination, positive incentives should be considered.

Increase awareness of the need for cyber resilience across the sector, including among electricity-related institutions and authorities, among policymakers, regulators, and industry.

7. Discussion and Conclusions

This work was supported through survey responses based on several individual interviews with representatives of key energy companies from the Upper Rhine Region (URR) as well as stakeholder workshops with electricity network operators. These helped to clarify their attitude towards energy decentralisation in terms of regional energy resilience via distributed renewable energy resources and their concerns, anticipated challenges, future plans and development perspectives.

The power system transition to smart grids introduces challenges into the development of electricity distribution networks. Considering the fact that stakeholders and actors' interest within the market should be always guaranteed for obtaining a successful electricity network upgrade, their opinion and experience is very valuable insight for policy maker in this sector. Especially when it comes to the most pertinent technological problematics arising mainly from the various distributed energy resources (DERs) integration and use as well as network optimization and security[10].

To improve the cyber resilience of electricity systems, policymakers must first raise awareness and collaborate with stakeholders to continuously identify, manage, and communicate emerging vulnerabilities and hazards. Policymakers are also in a unique position to foster cross-sector collaboration, organize information exchange programs, and support research initiatives in the electrical industry and beyond. Ecosystem-wide collaboration can aid in better understanding of the dangers that each stakeholder poses to the ecosystem, as well as vice versa.

There are a plethora of risk management tools, security frameworks, technical solutions, and self-assessment methodologies to choose from. Policymakers and business leaders must use what is relevant in their situation and view resilience as an ongoing process rather than a one-time event. Both policymakers and industry should commit to a collaborative approach based on constant conversation.

While complete prevention of cyberattacks is impossible, electricity systems can be made more cyber resilient by designing them to withstand shocks and be able to quickly absorb, recover, or adapt, all while maintaining the continuity of critical infrastructure operations, or at least a large part of it. It's crucial to be able to adapt to new technology, as well as new hazards and threats.

Governments all across the world can improve cyber resilience through a variety of policies and regulations, ranging from highly prescriptive to framework-oriented, performance-based methods. More prescriptive approaches have the benefit of allowing for more efficient compliance monitoring, but they may struggle to keep up with developing cyber threats. Less prescriptive, framework-based approaches allow for diverse approaches and implementation speeds across jurisdictions, but also raise challenges about how to develop a coherent and strong cross-border cybersecurity approach that has a demonstrable and effective impact. While taking into account the global character of risks, implementation techniques should be adjusted to national situations[11].

Because of the global and fast nature of the internet, international cooperation is especially vital — an attack on a single asset can quickly spread across the globe. International organizations and policymakers play a critical role in developing international collaboration. Collaboration across all key stakeholder groups, from senior policymakers and regulators to individual utilities and electrical equipment providers, should be a priority.

In the ENISA report about the NIS Investment in November 2021[12], a survey of 947 organisations identified as Operators of Essential Services (OES) and Digital Service Providers (DSP) across the 27 Member States has been conducted.

The results indicated that 48.9 % of surveyed affirm the significant positive impact adduced by the NIS Directive on information security in their field. While almost half of them believe that it has strengthened their detection capabilities, only 26 % has reported any improvements on the recovery aspect.

The vast majority of them has also stated that broadly their information security controls meet or exceed industry standards. Nevertheless, a strong link between a high self-perception of cybersecurity maturity and the presence of cybersecurity certifications for processess, people, and products within a company was perceived.

However, from a financial point of view most of the participants (67 %) have stressed the fact that the execution of the NIS Directive necessitated a separate budget, estimated at a median cost of EUR 40 000, or the equivalent to 5.1% of their overall information security budgets besides requiring additional full-time employees.

8. References

[1] Energy Expert Cyber Security Platform, “Recommendations for the European Commission on a European Strategic Framework and Potential Future Legislative Acts for the Energy Sector,” *EECSP Rep.*, no. February, p. 74, 2017.

[2] D. Frieden, A. Tuerk, C. Neumann, S. D’Herbemont, and J. Roberts, “Collective self-consumption and energy communities : Trends and challenges in the transposition of the EU framework,” *Compile*, no. December, pp. 1–50, 2020.

[3] C. Inês, P. L. Guilherme, M. G. Esther, G. Swantje, H. Stephen, and H. Lars, “Regulatory challenges and opportunities for collective renewable energy prosumers in the EU,” *Energy Policy*, vol. 138, no. December 2019, 2020, doi: 10.1016/j.enpol.2019.111212.

[4] German Federal Parliament, *Renewable Energy Sources Act (EEG 2017)*. 2009, pp. 5–31.

[5] “» Federal Immission Control Act (Bundes-Immisionsschutzgesetz, BImSchG) – Excerpts German Law Archive.” https://germanlawarchive.iuscomp.org/?p=315 (accessed Apr. 25, 2022).

[6] IEA, “Federal States (Länder) Support for Renewable Energy – Policies - IEA.” https://www.iea.org/policies/4058-federal-states-lander-support-for-renewable-energy (accessed Apr. 25, 2022).

[7] “La transition écologique et solidaire vers la neutralité carbone Mars 2020”.

[8] K. Löffler, T. Burandt, K. Hainsch, P. Y. Oei, F. Seehaus, and F. Wejda, “Chances and barriers for

Germany’s low carbon transition - Quantifying uncertainties in key influential factors,” *Energy*, vol. 239, 2022, doi: 10.1016/j.energy.2021.121901.

[9] International Energy Agency and RTE, “Conditions and Requirements for the Technical Feasibility of a Power System with a High Share of Renewables in France Towards 2050,” 2021. doi: 10.1787/6be9f3ac-en.

[10] K. H. Sirviö, H. Laaksonen, K. Kauhaniemi, and N. Hatziargyriou, “Evolution of the Electricity Distribution Networks—Active Management Architecture Schemes and Microgrid Control Functionalities,” *Appl. Sci. 2021, Vol. 11, Page 2793*, vol. 11, no. 6, p. 2793, Mar. 2021, doi: 10.3390/APP11062793.

[11] J. Marron, A. Gopstein, N. Bartol, and V. Feldman, “Cybersecurity framework smart grid profile,” Jul. 2019, doi: 10.6028/NIST.TN.2051.

[12] European Union Agency for Cybersecurity, “Nis Investments,” 2021. doi: 10.2824/77127.